

116TH CONGRESS
2D SESSION

S. 5008

To require notification of incidents at agencies involving sensitive personal information, and for other purposes.

IN THE SENATE OF THE UNITED STATES

DECEMBER 10, 2020

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To require notification of incidents at agencies involving sensitive personal information, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Federal System Inci-
5 dent Response Act of 2020”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) APPROPRIATE CONGRESSIONAL COMMIT-
9 TEES.—The term “appropriate congressional com-
10 mittees” means—

1 (A) the Committee on Homeland Security
2 and Governmental Affairs of the Senate;

3 (B) the Committee on Oversight and Re-
4 form of the House of Representatives; and

5 (C) the Committee on Homeland Security
6 of the House of Representatives.

7 (2) DIRECTOR.—The term “Director” means
8 the Director of the Office of Management and Budg-
9 et.

10 **SEC. 3. FEDERAL INFORMATION SYSTEM INCIDENT RE-**
11 **SPONSE.**

12 (a) IN GENERAL.—Chapter 35 of title 44, United
13 States Code, is amended by adding at the end the fol-
14 lowing:

15 **“Subchapter IV—Federal Information System**
16 **Incident Response**

17 **“§ 3591. Definitions**

18 “(a) IN GENERAL.—Except as provided under sub-
19 section (b), the definitions under section 3502 shall apply
20 to this subchapter.

21 “(b) ADDITIONAL DEFINITIONS.—As used in this
22 subchapter:

23 “(1) APPROPRIATE NOTIFICATION ENTITIES.—
24 The term ‘appropriate notification entities’ means—

1 “(A) the Committee on Homeland Security
2 and Governmental Affairs of the Senate;

3 “(B) the Committee on Commerce,
4 Science, and Transportation of the Senate;

5 “(C) the Committee on Oversight and Re-
6 form of the House of Representatives;

7 “(D) the Committee on Homeland Security
8 of the House of Representatives;

9 “(E) the Committee on Science, Space,
10 and Technology of the House of Representa-
11 tives;

12 “(F) the appropriate authorization and ap-
13 propriations committees of Congress;

14 “(G) the Director;

15 “(H) the Secretary of Homeland Security;
16 and

17 “(I) the Comptroller General of the United
18 States.

19 “(2) INCIDENT.—The term ‘incident’ has the
20 meaning given the term in section 3552 of this title.

21 “(3) CONTRACTOR.—The term ‘contractor’—

22 “(A) means any person or business that
23 collects or maintains information that includes
24 personally identifiable information or sensitive

1 personal information on behalf of an agency;
2 and

3 “(B) includes any subcontractor of a per-
4 son or business described in subparagraph (A).

5 “(4) COVERED INCIDENT.—The term ‘covered
6 incident’ means, with respect to any information col-
7 lected or maintained by or on behalf of an agency
8 or information system used or operated by an agen-
9 cy or by a contractor of an agency or other organiza-
10 tion on behalf of an agency—

11 “(A) a major incident, as defined by the
12 Director pursuant to section 2(b) of the Federal
13 Information Security Modernization Act of
14 2014 (44 U.S.C. 3554 note);

15 “(B) any incident determined likely to
16 have a significant impact on national security,
17 homeland security, or economic security of the
18 United States;

19 “(C) any incident determined likely to have
20 a significant impact on the operations of the
21 agency or the Federal Government; or

22 “(D) any incident that is determined to
23 have involved any sensitive personal informa-
24 tion, regardless of the number of impacted indi-
25 viduals.

1 “(5) INTELLIGENCE COMMUNITY.—The term
2 ‘intelligence community’ has the meaning given the
3 term in section 3 of the National Security Act of
4 1947 (50 U.S.C. 3003).

5 “(6) NATIONWIDE CONSUMER REPORTING
6 AGENCY.—The term ‘nationwide consumer reporting
7 agency’ means a consumer reporting agency de-
8 scribed in section 603(p) of the Fair Credit Report-
9 ing Act (15 U.S.C. 1681a(p)).

10 “(7) SENSITIVE PERSONAL INFORMATION.—
11 The term ‘sensitive personal information’ means,
12 with respect to an individual—

13 “(A) any combination of data or informa-
14 tion that, if exposed, could result in substantial
15 harm, physical harm, embarrassment, or unfair-
16 ness to the individual, including biometric, ge-
17 netic, or other data; and

18 “(B) any other information as determined
19 by the Director.

20 “(8) SUBSTANTIAL HARM.—The term ‘substan-
21 tial harm’, with respect to an individual, means iden-
22 tity theft, financial fraud, or other financial harm to
23 the individual.

1 **“§ 3592. Notification to impacted individuals involv-**
2 **ing sensitive personal information**

3 “(a) NOTIFICATION.—As expeditiously as practicable
4 and without unreasonable delay, and in any case not later
5 than 30 days after an agency has a reasonable basis to
6 conclude that a covered incident described in section
7 3591(b)(4)(D) has occurred, the head of the agency shall
8 provide notice of the incident in accordance with sub-
9 section (b) in writing to the last known home mailing ad-
10 dress of each impacted individual.

11 “(b) CONTENTS OF NOTICE.—Each notice required
12 under subsection (a) shall include—

13 “(1) a description of the categories of sensitive
14 personal information that were, or are reasonably
15 believed to have been, involved in the covered inci-
16 dent, including a list of all data elements;

17 “(2) a description of the substantial harm, em-
18 barrassment, inconvenience, or unfairness to the in-
19 dividual that an individual may reasonably expect to
20 experience based on the information or combination
21 of information involved in the covered incident;

22 “(3) contact information for the Federal Bu-
23 reau of Investigation or other appropriate entity;

24 “(4) the contact information of each nationwide
25 consumer reporting agency;

1 “(5) the contact information for questions to
2 the agency, including a telephone number, e-mail ad-
3 dress, and website;

4 “(6) information on any remedy being offered
5 by the agency;

6 “(7) consolidated Federal Government rec-
7 ommendations on what to do in the event of a cov-
8 ered incident; and

9 “(8) any other appropriate information as de-
10 termined by the head of the agency.

11 “(c) DELAY OF NOTIFICATION.—

12 “(1) IN GENERAL.—The Inspector General of
13 the agency that experienced the covered incident, the
14 Attorney General, the Director of National Intel-
15 ligence, or the Secretary of Homeland Security may
16 impose a delay of a notification required under sub-
17 section (a) if the notification would disrupt a law en-
18 forcement investigation, endanger national security,
19 or hamper security remediation actions.

20 “(2) DOCUMENTATION.—

21 “(A) IN GENERAL.—Any delay under para-
22 graph (1) shall be reported in writing to the
23 head of the agency, the Director, the Director
24 of the Cybersecurity and Infrastructure Secu-
25 rity Agency, and the Office of Inspector Gen-

1 eral of the agency that experienced the covered
2 incident.

3 “(B) CONTENTS.—A statement required
4 under subparagraph (A) shall include a written
5 statement from the entity that delayed the noti-
6 fication explaining the need for the delay.

7 “(C) FORM.—The statement required
8 under subparagraph (A) shall be unclassified,
9 but may include a classified annex.

10 “(3) RENEWAL.—A delay under paragraph (1)
11 shall be for a period of 2 months and may be re-
12 newed.

13 “(d) EXEMPTION FOR NOTIFICATION.—

14 “(1) IN GENERAL.—The head of an agency, in
15 consultation with the Inspector General of the agen-
16 cy, may request an exemption from the Director
17 from complying with the notification requirements
18 under subsection (a) if—

19 “(A) the information affected by the cov-
20 ered incident is determined by an independent
21 evaluation to be unreadable, including instances
22 when the information is encrypted or when the
23 encryption key has not been acquired; or

24 “(B) the covered incident has otherwise
25 been determined by an independent evaluation

1 to be of de minimis threat to those individuals
2 whose sensitive personal information was in-
3 volved in the incident.

4 “(2) APPROVAL.—The Director shall make a
5 determination for granting an exemption in con-
6 sultation with—

7 “(A) the Director of the Cybersecurity and
8 Infrastructure Security Agency; and

9 “(B) the Attorney General.

10 “(3) DOCUMENTATION.—Any exemption grant-
11 ed by the Director under subparagraph (A) or (B)
12 of paragraph (1) shall be reported in writing to the
13 head of the agency that experienced the covered inci-
14 dent, the Office of Inspector General of the agency
15 that experienced the covered incident, and the Direc-
16 tor of the Cybersecurity and Infrastructure Security
17 Agency.

18 “(e) UPDATE NOTIFICATION.—If an agency deter-
19 mines there is a change in the reasonable basis to conclude
20 that a covered incident occurred, or that there is a change
21 in the details of the information provided to impacted indi-
22 viduals as described in subsection (b), the agency shall as
23 expeditiously as practicable and without unreasonable
24 delay, and in any case not later than 30 days after such

1 a determination, notify all such individuals who received
 2 a notification pursuant to subsection (a) of those changes.

3 “(f) RULE OF CONSTRUCTION.—Nothing in this sec-
 4 tion shall be construed to limit—

5 “(1) the Director from issuing guidance regard-
 6 ing notifications or the head of an agency from
 7 sending notifications to individuals impacted by inci-
 8 dents not determined to be covered incidents, as de-
 9 scribed in section 3591(b)(4)(D); or

10 “(2) the Director from issuing guidance regard-
 11 ing notifications for covered incidents meeting the
 12 criteria in section 3591(b)(4)(D) or the head of an
 13 agency from issuing notifications to individuals im-
 14 pacted by covered incidents meeting the criteria in
 15 section 3591(b)(4)(D) that contain more information
 16 than described in subsection (b).

17 **“§ 3593. Congressional notifications and reports**

18 “(a) INITIAL REPORT.—

19 “(1) IN GENERAL.—Not later than 7 days after
 20 the date on which an agency has a reasonable basis
 21 to conclude that a covered incident occurred, the
 22 head of the agency shall submit a written notifica-
 23 tion and, to the extent practicable, provide a brief-
 24 ing, to the appropriate notification entities, taking
 25 into account the information known at the time of

1 the notification, the sensitivity of the details associ-
2 ated with the covered incident, and the classification
3 level of the information contained in the notification.

4 “(2) CONTENTS.—A notification required under
5 paragraph (1) shall include—

6 “(A) a summary of the information avail-
7 able about the covered incident, including how
8 the covered incident occurred, based on infor-
9 mation available to agency officials as of the
10 date which the agency submits the report;

11 “(B) if applicable, an estimate of the num-
12 ber of individuals impacted by the covered inci-
13 dent, including an assessment of the risk of
14 harm to impacted individuals based on informa-
15 tion available to agency officials on the date on
16 which the agency submits the report;

17 “(C) if applicable, a description and any
18 associated documentation of any circumstances
19 necessitating a delay in or exemption to notifi-
20 cation granted under subsection (c) or (d) of
21 section 3592; and

22 “(D) if applicable, an assessment of the
23 impacts to the agency, the Federal Government,
24 or the security of the United States as identi-
25 fied in section 3591(b)(4), based on information

1 available to agency officials on the date on
2 which the agency submits the report.

3 “(b) SUPPLEMENTAL REPORT.—Within a reasonable
4 amount of time, but not later than 45 days after the date
5 on which additional information relating to a covered inci-
6 dent for which an agency submitted a written notification
7 under subsection (a) is discovered by the agency, the head
8 of the agency shall submit to the appropriate congres-
9 sional committees updates to the written notification that
10 include summaries of—

11 “(1) the threats and threat actors,
12 vulnerabilities, means by which the covered incident
13 occurred, and impacts to the agency relating to the
14 covered incident;

15 “(2) any risk assessment and subsequent risk-
16 based security implementation of the affected infor-
17 mation system before the date on which the covered
18 incident occurred;

19 “(3) the status of compliance of the affected in-
20 formation system with applicable security require-
21 ments at the time of the covered incident;

22 “(4) an estimate of the number of individuals
23 affected by the covered incident based on informa-
24 tion available to agency officials as of the date on
25 which the agency submits the update;

1 “(5) an update to the assessment of the risk of
2 harm to impacted individuals affected by the covered
3 incident based on information available to agency of-
4 ficials as of the date on which the agency submits
5 the update;

6 “(6) an update to the assessment of the risk to
7 agency operations, or to impacts on other agency or
8 non-Federal entity operations, affected by the cov-
9 ered incident based on information available to agen-
10 cy officials as of the date on which the agency sub-
11 mits the update; and

12 “(7) the detection, response, and remediation
13 actions of the agency, including any support pro-
14 vided by the Cybersecurity and Infrastructure Secu-
15 rity Agency under section 3594(d) and status up-
16 dates on the notification process described in section
17 3592(a), including any delay or exemption described
18 in subsection (c) or (d), respectively, of section
19 3592, if applicable.

20 “(c) UPDATE REPORT.—If the agency determines
21 that there is any significant change in the scope, scale,
22 or consequence of the covered incident, or a change in the
23 inclusion of the criteria described in section 3591(b)(4),
24 the agency shall provide an updated report to the appro-

1 piate congressional committees that includes those
2 changes.

3 “(d) ANNUAL REPORT.—Each agency shall submit as
4 part of the annual report required under section
5 3554(c)(1) of this title a description of each covered inci-
6 dent that occurred during the 1-year period preceding the
7 date on which the report is submitted.

8 “(e) DELAY AND EXEMPTION REPORT.—The Direc-
9 tor shall submit to the appropriate notification entities an
10 annual report on all notification delays and exemptions
11 granted pursuant to subsections (c) and (d) of section
12 3592.

13 “(f) REPORT DELIVERY.—Any written notification or
14 report required to be submitted under this section may
15 be submitted in a paper or electronic format.

16 “(g) RULE OF CONSTRUCTION.—Nothing in this sec-
17 tion shall be construed to limit—

18 “(1) the ability of an agency to provide addi-
19 tional reports or briefings to Congress; or

20 “(2) Congress from requesting additional infor-
21 mation from agencies through reports, briefings, or
22 other means.

1 **“§ 3594. Government information sharing and inci-**
2 **dent response**

3 “(a) IN GENERAL.—The head of each agency shall
4 make available any information relating to an incident,
5 whether obtained by the Federal Government or a private
6 entity contracted by the Federal Government, to the Cy-
7 bersecurity and Infrastructure Security Agency, the De-
8 partment of Defense, and the Office of Management and
9 Budget to help mitigate future incidents.

10 “(b) COMPLIANCE.—The information made available
11 under subsection (a) shall—

12 “(1) take into account the level of classification
13 of the information and any information sharing limi-
14 tations relating to law enforcement; and

15 “(2) be in compliance with the requirements
16 limiting the release of information under section
17 552a of title 5 (commonly known as the ‘Privacy Act
18 of 1974’).

19 “(c) RESPONDING TO INFORMATION REQUESTS
20 FROM AGENCIES EXPERIENCING INCIDENTS.—An agency
21 that receives a request from another agency or Federal
22 entity for information specifically intended to assist in the
23 remediation or notification requirements due to an inci-
24 dent shall provide that information to the greatest extent
25 possible, in accordance with guidance issued by the Direc-
26 tor and taking into account classification, law enforce-

1 ment, national security, and compliance with section 552a
2 of title 5 (commonly known as the ‘Privacy Act of 1974’).

3 “(d) INCIDENT RESPONSE.—Each agency that has a
4 reasonable basis to conclude that a covered incident oc-
5 curred, regardless of delays or exemptions from notifica-
6 tion granted for a covered incident, shall consult with the
7 Cybersecurity and Infrastructure Security Agency regard-
8 ing—

9 “(1) incident response and recovery; and

10 “(2) recommendations for mitigating future in-
11 cidents.

12 **“§ 3595. Responsibilities of contractors and grant re-**
13 **cipients**

14 “(a) NOTIFICATION.—

15 “(1) IN GENERAL.—Subject to paragraph (3),
16 any contractor of an agency or recipient of a grant
17 from an agency that has a reasonable basis to con-
18 clude that an incident involving Federal information
19 has occurred shall immediately notify the agency.

20 “(2) PROCEDURES.—

21 “(A) COVERED INCIDENT.—Following no-
22 tification of a covered incident by a contractor
23 or recipient of a grant under paragraph (1), an
24 agency, in consultation with the contractor or
25 grant recipient, as applicable, shall carry out

1 the requirements under sections 3592, 3593,
2 and 3594 with respect to the covered incident.

3 “(B) INCIDENT.—Following notification of
4 an incident by a contractor or recipient of a
5 grant under paragraph (1), an agency, in con-
6 sultation with the contractor or grant recipient,
7 as applicable, shall carry out the requirements
8 under section 3594 with respect to the incident.

9 “(3) APPLICABILITY.—This subsection shall
10 apply to a contractor of an agency or a recipient of
11 a grant from an agency that—

12 “(A) receives information from the agency
13 that the contractor or recipient, as applicable, is
14 not contractually authorized to receive;

15 “(B) experiences an incident relating to
16 Federal information on an information system
17 of the contractor or recipient, as applicable; or

18 “(C) identifies an incident involving a Fed-
19 eral information system.

20 “(b) INCIDENT RESPONSE.—Any contractor of an
21 agency or recipient of a grant from an agency that has
22 a reasonable basis to conclude that a covered incident oc-
23 curred shall, in coordination with the agency, consult with
24 the Cybersecurity and Infrastructure Security Agency re-
25 garding—

1 “(1) incident response assistance; and

2 “(2) recommendations for mitigating future in-
3 cidents at the agency.

4 “(c) EFFECTIVE DATE.—This section shall apply on
5 and after the date that is 1 year after the date of enact-
6 ment of the Federal System Incident Response Act of
7 2020.

8 **“§ 3596. Training**

9 “(a) IN GENERAL.—Each agency shall develop train-
10 ing for individuals at the agency with access to Federal
11 information or information systems on how to identify and
12 respond to an incident, including—

13 “(1) the internal process at the agency for re-
14 porting an incident; and

15 “(2) the obligation of the individual to report to
16 the agency not only a confirmed covered incident,
17 but also a suspected incident, involving information
18 in any medium or form, including paper, oral, and
19 electronic.

20 “(b) APPLICABILITY.—The training developed under
21 subsection (a) shall—

22 “(1) be required for an individual before the in-
23 dividual may access Federal information or informa-
24 tion systems; and

1 “(2) apply to individuals with temporary access
 2 to Federal information or information systems, such
 3 as detailees, contractors, subcontractors, grantees,
 4 volunteers, and interns.

5 “(c) INCLUSION IN ANNUAL TRAINING.—The train-
 6 ing developed under subsection (a) may be included as
 7 part of an annual privacy or security awareness training
 8 of the agency, as applicable.

9 **“§ 3597. Analysis and report on Federal incidents**

10 “(a) ANALYSIS OF FEDERAL INCIDENTS.—

11 “(1) IN GENERAL.—The Director of the Cyber-
 12 security and Infrastructure Security Agency shall
 13 perform continuous monitoring of incidents of Fed-
 14 eral information systems.

15 “(2) QUANTITATIVE AND QUALITATIVE ANAL-
 16 YSES.—The Director of the Cybersecurity and Infra-
 17 structure Security Agency, in consultation with the
 18 Director, shall develop and perform quantitative and
 19 qualitative analyses of incidents of Federal informa-
 20 tion systems, including—

21 “(A) the causes of incidents, including—

22 “(i) attacker tactics, techniques, and
 23 procedures; and

1 “(ii) system vulnerabilities, including
2 zero days, unpatched systems, and infor-
3 mation system misconfigurations;

4 “(B) the scope and scale of incidents with-
5 in the agency networks and systems;

6 “(C) cross Federal Government root causes
7 of incidents;

8 “(D) agency response, recovery, and reme-
9 diation actions and effectiveness of incidents;
10 and

11 “(E) lessons learned and recommendations
12 in responding, recovering, remediating, and
13 mitigating future incidents.

14 “(3) SHARING OF ANALYSIS.—The Director
15 shall share on an ongoing basis the analyses re-
16 quired under this subsection with Federal agencies.

17 “(b) REPORT ON FEDERAL INCIDENTS.—Not later
18 than 2 years after the date of enactment of this section,
19 and not less frequently than every year thereafter, the Di-
20 rector of the Cybersecurity and Infrastructure Security
21 Agency, in consultation with the Director and the Director
22 of the Federal Bureau of Investigation, shall submit to
23 the appropriate congressional committees a report that in-
24 cludes—

1 “(1) a summary of causes of incidents from
2 across the Federal Government; and

3 “(2) the quantitative and qualitative analyses of
4 incidents developed under subsection (a)(2).

5 “(c) PUBLICATION.—A version of each report sub-
6 mitted under subsection (b) shall be made publicly avail-
7 able on the website of the Cybersecurity and Infrastruc-
8 ture Security Agency during the year in which the report
9 is submitted.

10 “(d) INFORMATION PROVIDED BY AGENCIES.—The
11 analysis required under subsection (a) and each report
12 submitted under subsection (b) shall utilize information
13 provided by agencies pursuant to section 3594(d).

14 “(e) REQUIREMENT TO ANONYMIZE INFORMA-
15 TION.—In sharing the analysis required under subsection
16 (a) and preparing each report under subsection (b), the
17 Director of the Cybersecurity and Infrastructure Security
18 Agency shall sufficiently anonymize and compile informa-
19 tion such that no specific incidents of an agency can be
20 identified, except with the concurrence of the Director of
21 the Office of Management and Budget.”.

22 (b) RESPONSIBILITIES OF THE CYBERSECURITY AND
23 INFRASTRUCTURE SECURITY AGENCY.—

24 (1) RECOMMENDATIONS.—Not later than 180
25 days after the date of enactment of this Act, the Di-

1 rector of the Cybersecurity and Infrastructure Secu-
2 rity Agency, in coordination with the Director of the
3 Federal Trade Commission, the Director of the Se-
4 curities and Exchange Commission, the Secretary of
5 the Treasury, the Director of the Federal Bureau of
6 Investigation, the Director of the National Institute
7 of Standards and Technology, and the head of any
8 other appropriate Federal or non-Federal entity,
9 shall consolidate, maintain, and make publicly avail-
10 able recommendations for individuals whose sensitive
11 personal information, as defined in section 3591 of
12 title 44, United States Code, as added by this Act,
13 is inappropriately exposed.

14 (2) PLAN FOR ANALYSIS OF, AND REPORT ON,
15 FEDERAL INCIDENTS.—

16 (A) IN GENERAL.—Not later than 180
17 days after the date of enactment of this Act,
18 the Director of the Cybersecurity and Infra-
19 structure Security Agency shall—

20 (i) develop a plan for the development
21 of the analysis required under section
22 3597(a) of title 44, United States Code, as
23 added by subsection (a), and the report re-
24 quired under subsection (b) of that section
25 that includes—

1 (I) a description of any chal-
2 lenges the Director anticipates en-
3 countering; and

4 (II) the use of automation for
5 collecting, compiling, monitoring, and
6 analyzing data; and

7 (ii) provide to the appropriate con-
8 gressional committees a briefing on the
9 plan developed under clause (ii).

10 (B) BRIEFING.—Not later than 1 year
11 after the date of enactment of this Act, the Di-
12 rector of the Cybersecurity and Infrastructure
13 Security Agency shall provide to the appro-
14 priate congressional committees a briefing on—

15 (i) the execution of the plan required
16 under subparagraph (A); and

17 (ii) the development of the report re-
18 quired under section 3597(b) of title 44,
19 United States Code, as added by this Act.

20 (c) RESPONSIBILITIES OF THE DIRECTOR OF THE
21 OFFICE OF MANAGEMENT AND BUDGET.—

22 (1) FISMA.—Section 2(b) of the Federal Infor-
23 mation Security Modernization Act of 2014 (44
24 U.S.C. 3554 note) is amended to read as follows:

25 “(b) MAJOR INCIDENT.—

1 “(1) IN GENERAL.—The Director of the Office
2 of Management and Budget shall develop guidance
3 on what constitutes a major incident for purposes of
4 section 3554(b) of title 44, United States Code, as
5 added by subsection (a).

6 “(2) EVALUATION AND UPDATES.—Not later
7 than 2 years after the date of enactment of the Fed-
8 eral System Incident Response Act of 2020, and not
9 less frequently than every 2 years thereafter, the Di-
10 rector of the Office of Management and Budget
11 shall submit to the Committee on Homeland Secu-
12 rity and Governmental Affairs of the Senate and the
13 Committee on Oversight and Reform of the House
14 of Representatives an evaluation, which shall in-
15 clude—

16 “(A) an update, if necessary, the definition
17 of a major incident, as defined by the Director
18 pursuant to section 3554(b) of this title;

19 “(B) the criteria of an incident that des-
20 ignates such an incident as a major incident;

21 “(C) an explanation for the analysis lead-
22 ing to the criteria in subparagraph (B); and

23 “(D) an assessment of any additional
24 datasets that may be considered sensitive per-

sonal information, as defined in section 3591 of this title.”.

(2) INCIDENT DATA SHARING.—

(A) IN GENERAL.—The Director shall develop guidance, to be updated not less than frequently every 2 years, on the content and format of the data to be made available by agencies pursuant to section 3594(a) of title 44, United States Code, as added by this Act.

(B) REQUIREMENTS.—The guidance developed under subparagraph (A) shall—

(i) prioritize data availability necessary to understand and analyze—

(I) the causes of incidents, as defined in section 3591 of title 44, United States Code, as added by this Act;

(II) the scope and scale of incidents within the agency networks and systems;

(III) cross Federal Government root causes of incidents; and

(IV) agency response, recovery, and remediation actions and effectiveness of incidents;

1 (ii) enable the efficient development
2 of—

3 (I) lessons learned and rec-
4 ommendations in responding, recov-
5 ering, remediating, and mitigating fu-
6 ture incidents; and

7 (II) the report of Federal inci-
8 dents pursuant to section 3597 of title
9 44, United States Code, as added by
10 this Act;

11 (iii) include requirements for the time-
12 liness of data availability; and

13 (iv) include requirements for using
14 automation for data sharing and avail-
15 ability.

16 (3) DEFINITION GUIDANCE.—Not later than 1
17 year after the date of enactment of this Act, the Di-
18 rector, in coordination with the Director of the
19 Cybersecurity and Infrastructure Security Agency
20 and in consultation with the Privacy and Civil Lib-
21 erties Oversight Board, shall develop guidance, to be
22 reviewed and, if necessary, updated not less fre-
23 quently than once every 2 years, on the interpreta-
24 tion of the terms “substantial harm”, “physical
25 harm”, “embarrassment”, or “unfairness to an indi-

vidual”, as used in the definition of the term “sensitive personal information” in section 3591 of title 44, United States Code, as added by this Act.

(4) STANDARD GUIDANCE AND TEMPLATES.—

Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Director of the Cybersecurity and Infrastructure Security Agency, shall develop guidance and templates, to be reviewed and, if necessary, updated not less frequently than once every 2 years, for use by Federal agencies in the activities required under sections 3592, 3593, and 3596 of title 44, United States Code, as added by this Act.

(5) CONTRACTOR AND GRANTEE GUIDANCE.—

(A) IN GENERAL.—Not later than 1 year after the date of enactment of this Act, the Director, in coordination with the Secretary of Homeland Security, the Secretary of Defense, the Administrator of General Services, and the heads of other agencies determined appropriate by the Director, shall issue guidance to Federal agencies on how to deconflict existing regulations, policies, and procedures relating to the responsibilities of contractors and grant recipi-

1 ents established under section 3595 of title 44,
2 United States Code, as added by this Act.

3 (B) EXISTING PROCESSES.—To the great-
4 est extent practicable, the guidance issued
5 under subparagraph (A) shall allow contractors
6 and grantees to utilize existing processes for no-
7 tifying Federal agencies of incidents involving
8 information of the Federal Government.

9 (6) UPDATED BRIEFINGS.—Not less frequently
10 than once every 2 years, the Director shall provide
11 to the appropriate congressional committees an up-
12 date on the guidance and templates developed under
13 paragraphs (2), (3), and (4).

14 (d) UPDATE TO THE PRIVACY ACT OF 1974.—Sec-
15 tion 552a(b) of title 5, United States Code (commonly
16 known as the “Privacy Act of 1974”) is amended—

17 (1) in paragraph (11), by striking “or” at the
18 end;

19 (2) in paragraph (12), by striking the period at
20 the end and inserting “; and”; and

21 (3) by adding at the end the following:

22 “(13) to another agency in furtherance of a re-
23 sponse to an incident (as defined in section 3552 of
24 title 44) and pursuant to the information sharing re-
25 quirements in section 3594 of title 44 if the head of

1 the requesting agency has made a written request to
 2 the agency that maintains the record specifying the
 3 particular portion desired and the activity for which
 4 the record is sought.”.

5 (e) TECHNICAL AND CONFORMING AMENDMENT.—
 6 The table of sections for chapter 35 of title 44, United
 7 States Code, is amended by adding at the end the fol-
 8 lowing:

“SUBCHAPTER IV—FEDERAL INFORMATION SYSTEM INCIDENT RESPONSE

“3591. Definitions.

“3592. Notification to impacted individuals involving sensitive personal informa-
 tion.

“3593. Congressional notifications and reports.

“3594. Government information sharing and incident response.

“3595. Responsibilities of contractors and grant recipients.

“3596. Training.

“3597. Analysis and report on Federal incidents.”.

